

Tilburg University

Data protection as bundles of principles, general rights, concrete subjective rights and rules

de Hert, Paul

Published in:
European Data Protection Law Review

DOI:
<https://doi.org/10.21552/edpl/2017/2/6>

Publication date:
2017

[Link to publication in Tilburg University Research Portal](#)

Citation for published version (APA):
de Hert, P. (2017). Data protection as bundles of principles, general rights, concrete subjective rights and rules: Piercing the veil of stability surrounding the principles of data protection. *European Data Protection Law Review*, 3(2), 160-179. <https://doi.org/10.21552/edpl/2017/2/6>

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal

Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Data Protection as Bundles of Principles, General Rights, Concrete Subjective Rights *and* Rules. Piercing the Veil of Stability Surrounding the Principles of Data Protection

Paul De Hert*

After having reflected about technologies and the role of non-political guidance in EU data protection law in previous editorials, I now turn to the thorny question about the proper place of data protection law. In search of a substance, I use Murakami's imaginary to prepare for the worst: not all things, concepts and beings are blessed with substance. After having managed (lowered) possible expectations about the essence of data protection law, I turn to a first approach to understanding data protection law as a bundle of principles. Principles are powerful legal topoi that create seriousness about legal domains. They are defended by the best scholars and much appreciated by courts in their role as judicial lawmakers. They look God-given, but are man-made. Unable to fix their number and precise nature, I will challenge them by inflating their number. A next editorial will do what this contribution fails to do: finding some substance in a principled-based law domain. Also it will look at another approach of understanding data protection via core values.

Murakami and Wild Geese That Fly with the Moon on Their Wings

Haruki Murakami's fictional world (*The Wind-Up Bird Chronicle*, *IQ84*, *Hard Boiled Wonderland*, *Sputnik Sweetheart* and *Kafka on the Shore*, etc) pleases not all, but many. Riddles are left unsolved, story lines and plots are not always fully developed and some of the strange imaginary lacks clear, rational or empirical coherent meaning. Trying to bring this author in a legal conversation therefore seems quite daring, guaranteeing that like fashionable knitwear that quickly becomes outdated at the end of the trend, so will my Murakami parallel sound passé when the next international literature hype imposes itself.

Still, there is no shame in being seduced by the author's dreamy nonconformists and his understanding of food, jazz and other Western music. In *Kafka on the Shore*, one of the two protagonists, the disturbingly young (15 years old) Kafka Tamura explores the Shikoku deep woods while listening to Coltrane's 'My favorite things'. The long

* Paul De Hert is full professor at the Vrije Universiteit Brussels (LSTS) and associated professor at Tilburg University (TILT).
DOI: 10.21552/edpl/2017/2/6

and dangerous walk turns out to be a journey of the highest importance in the young man's life bringing him to a parallel world where he finds some of the answers to questions with which he is struggling. If writing PhDs in law needs musical backing, Coltrane's study of the the Rodgers and Hammerstein anthem that we know from *The Sound of Music* has no equal (at least in my memories), by replacing tong breaking lyrics (cream-colored ponies, crisp apple strudels, flying wild geese, etc) with one long soprano sax meditation of endless duration.

In all Murakami novels, the male protagonist finds time to open up to other worlds - either by drastically changing his life style (running away, losing jobs, ...), or by organising his life so that it fits society superficially but still allows for space to reflect and wait for things to happen. Murakami's other worlds (present in most of his writings) only open up when these psychological requirements are met and we bond with the protagonists for their generosity in taking us with them when crossing.

Shapeless Concepts, Living Positive and Negative Spirits and Empty Shells

A closer look and an awareness of the existence of these other worlds reveal that we do not look well enough when interacting in this world: 'Our' world is in fact populated by a multitude of both non-humans or humans-that-partly-have-been. The non-humans are not easily categorised, especially not in *Kafka on the Shore* where UFOs appear and evil beings creep out of the mouth of dead bodies, but are never explained. More detail is given about the funny Colonel Sanders, who kindly but with impatience explains to one of the characters that he is not human, is not Colonel Sanders, but a nameless and shapeless 'metaphysical, conceptual object', or 'concept' whose job is to check 'the correlation between different worlds, making sure things are in the right order'.¹

Closer to us are the humans-that-partly-have-been. All these characters have lost something (a memory, a parent, a lover, a gift such as the ability to write) and are all driven by dark melancholy.² In *Sputnik Sweetheart*, Miu sees herself in another apartment having sex with a man, a troubling experience that turns her hair white and makes her lose her sexuality. Later on in the story, more is lost by Miu upon which she does not color her hair any longer but shows the white. K, the protagonist, senses she is now an *empty shell*.³

In *Kafka on the Shore*, it is hard to identify amongst the main characters who is not a human-that-partly-has-been. Chapter 23, one of the more academic ones, contains a

1 Harry Murakami, *Kafka on the Shore* (First published in 2003, English translation published by Vintage 2005) ch 30, 372.

2 A sweeter, swooning version of that emotion permeates Murakami's readership. English seems to lack the term for *weemoed* (Dutch) or *Wehmut* (German).

3 'An empty shell. Those were the first words that sprang to mind. Miu was like an empty room after everyone's left. Something incredibly important (...) had disappeared from Miu for good. Leaving behind not life, but its absence. Not the warmth of something alive, but the silence of memory' (*Sputnik Sweetheart*, ch 16).

full reflection on *living spirits* in Japanese Medieval literature, people that acquire ghost like features (such as travelling through space and time) after negative experiences. These *living spirits*, always motivated by evil, are then contrasted with people that, motivated by love, die to turn into real spirits to save someone or to rebuild the world in a positive world. So a good spirit is a dead one, a bad spirit can be a living spirit. Is it then possible, to be both good and living as a spirit? Of course, Murakami does not clarify his view on this but some of the main characters might qualify for the status of living positive spirit (Nakata?, the 19-year-old Miss Saeki?, the 15-year-old Miss Saeki?). For Kafka Tamura, the 19-year-old Miss Saeki is 'like a spirit that's sprung from a happy encounter', the 50-something Miss Saeki still living is real but has 'lost forever' to the darkness 'brilliant energy' while the 15-year-old Miss Saeki that comes to Kafka in his dreams a night is 'her ghost'.⁴

Frustrating as the (lack of) academic clarity of this Chapter 23 might be, there is always the easier category of *empty shells* to denote the humans-that-partly-have-been in *Kafka on the Shore*. The label and the idea behind it surfaces, sometimes quite explicitly, in several paragraphs. Kafka Tamura, for instance, sees himself as a 'hollow man',⁵ and for that reasons choses to walk into a dangerous forest to (hopefully) become 'part of a brand new world'.⁶ Similar reflections about their lacking parts are made by the old child-optimistic Nakata (who talks with cats and talks about himself in the 3rd person) and the life-tired Miss Saeki:

'Miss Saeki?'

'Yes?' she replied.

'Actually I don't' have any memories either. I'm stupid, you see, so could you tell me what memories are like?'

Miss Saeki stared at her hands on the desk, then looked up at Nakata again. 'Memories warm you up from the inside. But they can also tear you apart.'

Nakata shook his head. 'That's a rough one. Nakata still doesn't understand. The only thing I understand is the present.'

'I'm the exact opposite,' Miss Saeki said.⁷

Nakata and Not Understanding the Difference between Right or Wrong

This moving dialogue between Nakata and Miss Saeki sheds light (rather late in the novel) on some of the features of and differences between humans-that-partly-have-

4 'What I saw here in this room the night before was definitely Miss Saeki at 15. The *real* Miss Saeki, of course, is still alive. A 50-something woman, living a real life in the real world. Even now, she's in her room upstairs at her desk (...) but none of that changes the fact that what I saw here was her *ghost*. Oshima told me people can't be in two places at once, but I think it's possible. In fact, I'm *sure* of it. While they're still alive, people can become ghosts' (*Kafka on the Shore*, ch 23, 294).

5 See ch 41: 'Alone in such a dense forest, the person called *me* feels empty, horrible empty. Oshima once used the term "hollow men". Well that is what I've become. There is a void inside me, a blank that's slowly expanding devouring what's left of who I am. I can hear it happening. I am totally lost, my identity is dying' (ibid 508) and 'I head into the heart of the forest, a hollow man, a void that devours all that's substantial. So there I nothing left to fear. Not a thing' (ibid 509).

6 Murakami, *Kafka on the Shore* (n 1) ch 49.

7 ibid ch 42, 511.

been. Loneliness seems to be a common feature, illustrated by the lack of friends or memories or, on the contrary, the over-presence of memories.

Intriguing is Nakata's ability to self-reflect. Pretending to be stupid and not-knowing about many things, the old man is capable of calling by name that which he does not know (memories, desires) and to contrast it with things he does know:⁸

'Miss Saeki,' Nakata said, 'I only have half a shadow. The same as you'
'I know'

'Nakata lost it during that war. I don't know why that had to happen, and why it had to be me...

(...)

'Nakata doesn't know about sexual desire. Just as I don't have memories. I don't have any desire. So I don't understand the difference between right or wrong sexual desire. But if something did happen, it happened. Whether it's right or wrong, I accept everything that happens, and that's how I became the person I am now.'⁹

Clearly, a person like Nakata is much needed in this world. Many people (normal humans) turn to him to track their lost cats. But also humans-that-partly-have-been turn to him. Kafka Tamura uses Nakata in a dream to kill his father and Miss Saeki has patiently waited for him to finally leave this world for another one. Nakata can be used to alter the mechanisms of this real, physical world and, simultaneously, is himself capable of handling 'the entrance stone' that connects this world with the other world(s).

In other novels, the role of Nakata is played by female characters (for instance Creta Kano in *The Wind-Up Bird Chronicle* and Fuka-Eri in *IQ84*) and sex rather than entrance stones makes transitions to the other world possible.¹⁰ All these remarkable female Murakami creations, like Nakata, 'do not know about sexual desire' or desires in general.¹¹

How Murakami Transcends in This Foreword

Being quite pressured by the editor of this wonderful legal journal not to forget about the promised series of forewords on data protection and privacy, I completely mis-read several paragraphs of *Kafka on the Shore* and ended up with messages like these:

8 There is something of Murakami in Nakata, as the author himself in a 2004 interview, confesses that he is a loner (ibid 346), seeking to be humble (ibid 342) never chooses a story or what is going to happen but waits for the story to come (ibid 341) and prefers to be an observer rather than a judge ('I would like to leave everything wide open to all the possibilities in the world' ibid 347). John Wray, 'Interview with Haruki Murakami' (2004) reprinted in *The Paris Review* (vol 4, Picador 2009) 335-371.

9 Murakami, *Kafka on the Shore* (n 1) ch 42, 512.

10 On the role of sex and people functioning as 'mediums' in Murakami's books, see Wray (n 8) 353-354.

11 See equally, Colonel Sanders' explanations to Hoshino about not being bothered by good or evil [Murakami, *Kafka on the Shore* (n 1) ch 30, 372].

Data Protection Law doesn't know about substance. Just as it does not have any core values, it does not know of any prohibitive bright-line rules. It does not have any desire to develop these. So it doesn't understand the difference between right or wrong. But if something did happen, it happened. Whether it's right or wrong, data protection accepts everything that happens, and that's how it became the legal domain it is now.

There were more messages that popped up, but this one in particular, was most compelling. It struggled to find it definitive formulation and was often clogged by a very similar one, that I find slightly less persuasive:

Data Protection Laws do not know about substance. Just as they do not have any core values, they do not know of any prohibitive bright-line rules. They do not have any desire to develop these. So they do not understand the difference between right or wrong. But if something did happen, it happened. Whether it's right or wrong, data protection laws accept everything that happens, and that's how they became the legal reference points in many areas today.

(I find the latter more cynical but not less accurate). This legal message, also the more cynical version, that I found in *Kafka on the Shore* contains some echoes of ideas developed in previous forewords in this journal.¹² The suggestion that data protection law is no more than an empty shell, is best taken seriously when inspired by an author that makes a case about the presence in our world and the value of empty shells. What could such a denominator mean in law? A bundle of rules without practical real life impact? A bundle of rules without coherence or principles? Law on paper that does not stir the imagination of the judiciary?¹³ Law without substance, unable to erect dykes to restrict certain dangerous data-processing practices and to raise awareness of the importance of privacy safeguards? These questions will be broached in a next foreword. In this contribution, I want to reflect about the fact that data protection has principles. This should not be a surprise, since these principles stand upright in all basic data protection texts. If we look more closely at these principles, could we then find substance?

Data Protection as a Bundle of Principles

All data protection lawyers by now are familiar with the principles of data protection law. Beyond technicalities, these allow a universal dialogue about confronting data

12 Paul De Hert, 'The Future of Privacy. Addressing Singularities to Identify Bright-Line Rules That Speak to Us' (2016) 2(4) EDPL 461-466 and Paul De Hert, 'Data Protection's Future without Democratic Bright Line Rules. Co-existing with Technologies in Europe after Breyer' (2017) 3(1) EDPL 1-15.

13 Compare, 'Another line of criticism relates to marginalisation of the judiciary; in many countries, the courts have played little, if any, direct role in developing and enforcing data privacy norms. This situation not only results in scarcity of authoritative guidance on the proper interpretation of the relevant legislation but contributes to the marginalisation of data privacy as a field of law' (Lee Bygrave, 'Privacy Protection in a Global Context – A Comparative Overview' (2004) 47 Scandinavian Studies in Law 319-348, 347 with ref to Lee Bygrave, 'Where have all the judges gone? Reflections on judicial involvement in developing data protection law' in Peter Wahlgren(ed), *IT och juristutbildning. Nordisk årsbok i rättsinformatik 2000* (Jure AB 2001) 113-125).

processing activities. Well known are the Council of Europe and OECD Principles, both proclaimed in September 1980.¹⁴ This is the OECD formulation of the Principles:¹⁵

Collection Limitation: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject (Principle 1).

Data Quality: personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date (Principle 2).

Purpose Specification: The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose (Principle 3).

Use Limitation: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except: a) with the consent of the data subject; or b) by the authority of law (Principle 4).

Security Safeguards: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data (Principle 5).

Openness: There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller (Principle 6).

Individual Participation: An individual should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended (Principle 7).

Accountability: A data controller should be accountable for complying with measures which give effect to the principles stated above (Principle 8).

14 On 17 September 1980, the Committee of Ministers of the Council of Europe (CoE) adopted the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, the first legally binding international instrument in data protection. The convention sought to establish basic principles of data protection, to reduce restrictions on transborder data flows on the basis of reciprocity and to bring about co-operation between national data protection authorities (DPAs). Parties to the convention are required to apply the principles in their domestic legislation. Six days later, on 23 September 1980, the OECD Council adopted its Guidelines on transborder data flows. Although efforts were made to minimise the differences, some do occur nevertheless. The OECD Guidelines are not legally binding, whereas the CoE convention is binding on those countries that ratify it. The CoE convention only applies to personal data that are 'automatically' processed, whereas the Guidelines are valid for the processing of data in general, irrespective of the particular technology employed. The OECD Guidelines, unlike the CoE convention, do not mention the need to establish national data protection authorities, a crucial requirement in European data protection rules. But, all in all, the principles formulated are similar.

15 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data <<http://www.oecd.org/sti/ieconomy/oecdguidelinesonthe protection of privacy and transborder flows of personal data.htm#part2>> accessed 18 July 2017.

These eight principles are enclosed in the second part of the 1980 OECD Guidelines ('Part Two. Basic Principles of National Application'). Lesser known is the third part of this foundational text, adding more internationally oriented principles ('Part Three. Basic Principles Of International Application: Free Flow and Legitimate Restrictions'). This part is organised in four paragraphs with rather concrete do's and don't's, but without clearly stating whether all of this is of a 'principles' nature and, if so, 'how much' principles are envisaged:

15. Member countries should take into consideration the implications for other Member countries of domestic processing and re-export of personal data.

16. Member countries should take all reasonable and appropriate steps to ensure that transborder flows of personal data, including transit through a Member country, are uninterrupted and secure.

17. A Member country should refrain from restricting transborder flows of personal data between itself and another Member country except where the latter does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation. A Member country may also impose restrictions in respect of certain categories of personal data for which its domestic privacy legislation includes specific regulations in view of the nature of those data and for which the other Member country provides no equivalent protection.

18. Member countries should avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data that would exceed requirements for such protection.

The whole set-up and lay-out of the document reveals a qualitative difference between the first group of principles (of 'national application') and the second group of principles of 'international application' that want to safeguard the international free flow of information as much as possible.

There are other ways of organising and representing data protection law, for instance by distinguishing between principles and rights, or between principles, rights and duties. I always liked the way the UK Data Protection Act 1998 is organised, first spelling out all the terms and rules and practicalities, then adding some instructive schedules to please the reader.¹⁶ The first schedule to the Data Protection Acts enumerates and explains eight principles of which one (the 6th Principle) relates to six data subject rights and of which another one (the 8th Principle) deals in a coherent way with the international principle.¹⁷

16 Data Protection Act 1998 <http://www.legislation.gov.uk/ukpga/1998/29/pdfs/ukpga_19980029_en.pdf> accessed 18 July 2017.

17 Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless (...) (Principle 1). Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes (Principle 2). Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed (Principle 3). Personal data shall be accurate and, where necessary, kept up to date (Principle 4). Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes (Principle 5). Personal data shall be processed in accordance with the six rights of data subjects under this Act (Principle 6). Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data (Principle 7). Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data (Principle 8).

These 1980 lists of both the Council of Europe and the OECD are familiar to us, as they gave way to similar lists in the 1995 EU Directive,¹⁸ the OECD 2013 Guidelines and the UN 1991 Guidelines. The two international organisations found these principles in the legal systems of some pioneering countries in Europe and in US law [the 1970 American Fair Credit Reporting Act, the 1973 Department of Health Education and Welfare (HEW) report on fair information practices (FIP)¹⁹ and the 1974 Privacy Act].

Turning to literature, one also finds an insistence on principles. Bygrave, while explaining data protection, identifies six core principles²⁰ and proceeds with the argument that there might be other principles in data protection law, but these six 'are central to it', *they are data protection law*.²¹ Before I take a closer look at Bygrave's approach, it seems useful to refresh some of the essentials on principles, rights and rules

What is This Thing Called a Principle Again and Is It Law?

In his attack against positivism, Ronald Dworkin extensively discusses the difference between rules and principles.²² Dworkin firstly recalls Hart's positivistic approach to law that identifies legal obligations as only deriving from legal *rules*, enacted according to specific procedures that account for their validity.²³

Dworkin challenges this positivistic approach by arguing that a better way to understand law should include not only rules but also more general standards such as policies and principles. All norms are according to Dworkin either rules or principles. Both exist. Rules are the more concrete instruments. They are conceived in an all-or-nothing fashion. They are either valid, and in that case they must be respected, or invalid. If there is a conflict of rules, a possible way to solve it is to envisage an exception to a certain rule.²⁴

Principles on the contrary are to be conceived in an 'optimising' perspective. They set an optimum standard, which has to be complied with, compatibly with the factual or

18 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 L 281/31.

19 US Department of Health, Education And Welfare, *Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems* (July 1973) <<http://epic.org/privacy/hew1973report>> accessed 18 July 2017.

20 See Lee A Bygrave, *Data Privacy Law, an International Perspective* (Oxford University Press 2014) 1-2: 'Personal data should be collected by fair and lawful means (*principles of fair and lawful processing*); The amount of personal data collected should be limited to what is necessary to achieve the purpose(s) for which the data is gathered and further processed (*principle of minimality*); Personal data should be collected for specified, legitimate purposes, and not used in ways that are incompatible with those purposes (*principle of purpose limitation*); Personal data should be relevant, accurate, and complete in relation to the purposes for which it is processed (*principle of data quality*); Personal data should be protected against unauthorized attempts to disclose, delete, change or exploit it (*principle of data security*); Processing of personal data should be transparent to, and capable of being influenced by, the data subject (*principle of data subject influence*)'.

21 *ibid* 2.

22 Ronald M Dworkin, 'The Model of Rules' (1967-1968) 35 U Chi L Rev 17.

23 *ibid* 17.

24 *ibid* 25.

legal situation.²⁵ If there is a conflict between principles, this does not necessarily mean that either of them is invalid. They both remain valid, and the solution to the concrete case must be given on the basis of a conditional priority between the two principles. The principle which has more ‘weight’ prevails.²⁶

Dworkin dismisses Hart’s claim that all what is not decided on the basis of rules is only an outcome of judges’ discretion to rely on extra-legal sources. Conversely, Dworkin retains that principles should be acknowledged as part of the law, and legal obligations can also derive directly from principles.

Gallant nuances this approach by stating that principles are normative statements which *may* or *may not* harden in rules of law, while legal rules themselves are always binding on relevant actors and are enforceable by courts or in general by government coercion.²⁷ The hardening perspective also explains why *most* rights might be considered as principles rather than rules. For Ola Zetterquist most rights are by nature more akin to principles than to rules. Her argument is that a right often needs to be balanced against other rights and are not applicable in an all-or-nothing fashion.²⁸ I do not necessarily agree with this argument that rights *often* needs to be balanced against other rights,²⁹ but I follow the characterisation of rights being closer to principles than to rules because of their lack of detail.

Today’s lawyers are very confident in Dworkin’s understanding of how law functions. A wealth of factors has contributed to a solid position for principles in our legal systems (the rise of fundamental rights obligations for instance) and for a more prominent rule for judges (the presence of European treaty provisions with a direct effect and of European courts being two of them) who use principles to clarify vague or conflicting rules or engage, with some restraint due to their position, in rule-making activity.

A fine example of rule-making is *Ryneš* (2014)³⁰ where the Court of Justice of the European Union (CJEU) imposed a strict understanding of the household exemption in

25 For a discussion of the optimisation thesis, see Robert Alexy, ‘On the Structure of Legal Principles’ (2000) 13(3) *Ratio Juris* 294-304, 295.

26 Alexy recalls in this respect the example of an accused who was unable to attend Court’s proceedings due to health reasons. In this case, he explains the principle of the respect of the right to life and to the inviolability of one’s body is opposed to the principles of the good administration of justice, which would require the presence of the accused during Court’s proceedings, and it is closely linked to the more general principle of the rule of law. In the specific case discussed by Alexy, the German Constitutional Court gave conditional priority to the right to life of the accused (Decision of the Federal Constitutional Court, *BVerfGE* vol 51, 324). This does not mean that the rule of law principle is invalid. On the contrary in a different factual context, for instance when the risk for the health of a witness, rather than of the accused is not high, and his or her presence in the Court is fundamental carry out cross-examination, rule of law concerns might as well prevail.

27 Kenneth S Gallant, *The Principle of Legality in International and Comparative Criminal Law* (Cambridge University Press 2009) 7.

28 Ola Zetterquist, ‘The Charter of Fundamental Rights and the European *Res Publica*’ in Giacomo Di Federico (ed), *The EU Charter of Fundamental Rights. From Declaration to Binding Instrument* (Springer 2011) 10. See also page 13: ‘The rights laid down in the Charter need to be balanced against each other. Rights are much like principles in the sense that they are not, like rules, applicable in an all-or-nothing fashion. It is possible to in some cases restrict, say the right of freedom of expression in the interest of the right to privacy and to still say that one respects both rights. The rights are potentially in conflict with each other but must both be guaranteed to a reasonable degree’.

29 Bart van der Sloot, ‘The Practical and Theoretical Problems with Balancing’ (2016) 23(3) *Maastricht Journal of European and Comparative Law* 439-459.

30 Case C-212/13 *František Ryneš v Úřad pro ochranu osobních údajů* (2014) ECLI:EU:C:2014:2428, para 30.

the Directive based on a teleological reading (the goals of the Directive) and plain text interpretation [the term ‘purely’ in Article 3(2) of the Directive].³¹

In this interpretative work principles come in handy as starting points or leads. The obvious example is *Google Spain* where the CJEU argued that its task was to enforce ‘the general principles of law’, a notion that includes all fundamental rights and on this basis found in the Data Protection Directive the right to be forgotten-rule,³² a rule that after the ruling was incorporated by the EU legislator in the GDPR. The case tells us a nice tale about dividing the legislative work within the EU where some of the hardening of rules is done by the judges and then taken over by the legislator.

The Seductiveness of Principles: Flexible and More Likely to Be Universal

Principles are more flexible than rules. Indeed, their balancing and conditional priority will vary according to the context. Therefore, they can provide more tailored solutions when compared to hard-core rules.³³

Moreover, principles being more abstract are more likely to be more universal, and they are more ‘exportable’ across different jurisdictions. Fundamental principles and rights like the presumption of innocence and privacy are recognised in international instruments such as the International Covenant on Civil and Political Rights. However, these principles can translate in very different rules in the different jurisdictions. Examples are to be found in all areas of law, including criminal law.³⁴ The move in EU data protection law from a Directive towards a Regulation can be understood in this light. The principle of free flow in the internal market required more hardened rules that are applicable in a similar way across the Union. Hence the necessity of a Regulation with more detailed provisions.

So, principles can bridge differences in legal regimes and pave the way for common understanding of things (and eventually more common rules). The example that comes to mind are again the 1980 OECD Guidelines. These Guidelines have been extraordinarily successful in inducing OECD member countries, and others too, to introduce legislation based on them.³⁵ Marc Rotenberg has observed

31 According to art 3(2) of the Directive, the Directive shall not apply to the processing of personal data ‘in the course of a purely personal or household activity’.

32 The CJEU held that those provisions of the Directive that ‘govern the processing of personal data liable to infringe fundamental freedoms, in particular the right to privacy, must necessarily be interpreted in the light of fundamental rights, which, according to settled case-law, form an integral part of the general principles of law whose observance the Court ensures and which are now set out in the Charter’ [Case C-131/12 *Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* (2014) ECLI:EU:C:2014:317, para 68].

33 See the example above on the variable equilibrium between the respect to right to life and the rule of law concerning the presence of the accused or of the witness during Court’s proceedings.

34 The rules on preventive detention represent an example of this. Implying the deprivation of liberty of persons who have not been finally convicted yet, preventive detention should be subject to strict limitations if one wants to abide to the principle of the presumption of innocence. Yet, the actual rules on the actual temporal limitations vary from jurisdiction to jurisdiction (according to Italian law the police can detain suspects up to two days – 48 hours, while in Denmark this is possible only for 6 hours).

35 See David Wright, Paul De Hert and Serge Gutwirth, ‘Are the OECD Guidelines at 30 showing their age?’ (2011) 54(2) Communications of the ACM 119-127. When the Guidelines were adopted 30 years ago, only about one-third of member countries had privacy legislation. Today nearly all OECD member countries have laws – most of which follow the principles of the Guidelines – and authorities to enforce those laws.

a remarkable convergence of privacy policies. Countries around the world, with very distinct cultural backgrounds and systems of governance, have adopted roughly similar approaches to privacy protection.³⁶

Although the actual implementation can vary widely,³⁷ the OECD Guidelines continue to have influence. The US Department of Homeland Security set out its privacy policy in a memorandum at the end of 2008. Included were eight principles that closely tracked those in the Guidelines, although the memo also refers to the fair information practices in the Privacy Act of 1974.

The most amazing achievement of the data protection principles is, in my view, to be found in a 2008 report of an EU and US high-level, advisory group (the so-called High Level Contact Group, HLCCG). The group agreed a set of core principles, acceptable as minimum standards when processing personal data for law enforcement purposes and exchanging them at a transnational level.³⁸ The work would eventually lead to the ‘Umbrella Agreement’, signed by the US and the EU on 2 June 2016 and finalised by decisions of the European Parliament and European Council in December 2017, which complements existing and future EU-US and Member State-US agreements between law enforcement authorities.³⁹ The Agreement is not without criticism but it takes away discrimination between US and EU data subjects. The former can have redress for data harm in the EU, the latter could not. With the Umbrella Agreement, EU citizens not resident in the USA now have the right to challenge in US courts the way in which their data is used under the agreement.

The Seductiveness of Rules: A Constitutionalist Perspective

The foregoing shows that principles bridge, even in the area of security! Admittedly, depending on the sensitiveness of the matter, the contrary might also be true. Namely, people might find it easier to agree on specific rules even if they do not agree on the general, moral principle. Sunstein speaks in this context of *incompletely theorised agreements*, referring to those situations where an agreement has been found

36 Marc Rotenberg, ‘Fair Information Practices and the Architecture of Privacy (What Larry Doesn’t Get)’ (2001) 1 Stanford Technology Law Review, para 47.

37 Actual implementation of the fair information practices and/or the eight OECD principles can vary widely at the statutory, regulatory or data controller level depending on the country, the data controller, the type of data, conflicting goals and other factors. For example, accountability can be met through many different mechanisms, including criminal or civil penalties; national or provincial supervisory officials; other administrative enforcement; various forms of self-regulation including industry codes and privacy seals; formal privacy policies; compliance audits; employee training; privacy officers at the data controller level; and other methods.

38 These principles covered 1. Purpose specification or limitation; 2. Integrity and data quality; 3. Proportionality; 4. Information security; 5. Special categories of personal information (sensitive data); 6. Accountability; 7. Independent and effective oversight; 8. Individual access and rectification; 9. Transparency and notice; 10. Redress; 11. Automated individual decisions; and 12. Restrictions on onward transfers to third countries.

39 Franziska Boehm, ‘Assessing the New Instruments in EU-US Data Protection Law for Law Enforcement and Surveillance Purposes’ (2016) 2(2) EDPL 178-190. The Umbrella Agreement can be found at <<https://www.justice.gov/opcl/DPPA/download>> and Eur-Lex: <<http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016PC0237>> [Proposal for a Council Decision on the conclusion, on behalf of the European Union, of an Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offenses, COM/2016/0237 final - 2016/0126 (NLE)].

at a greater level of particularity, on specific rules, rather than on abstract principles.⁴⁰ He makes the example of religious liberty. People may agree that it is important to protect religious liberty (rule), even if they disagree on the theory behind it (principle). The underlying principle can be either social peace, the need to respect equality and recognition of human dignity, or even mere utilitarianism.⁴¹ Another example might be people agreeing on transparency when personal data are processed, while disagreeing on why it has to be so (because of human rights, or because of consumer protection). Yet, the drawbacks of this approach are that by seeking agreement at all costs, the agreement itself might fall short of fairness. Indeed, principles allow for a deeper theoretical discussion that is inherently linked to the values lying behind them. Borrowing from Sidgwick's writings on ethical method, Sunstein observes that 'concrete judgements about particular cases can prove inadequate for morality or constitutional law'.⁴² Therefore, incompletely theorised agreements focussing on rules are undoubtedly a valuable interpretative tool to understand how decisions are often taken. Yet, if one wants to embrace a more normative perspective and ensure a moral and fair discussion, the agreement must necessarily be sought at a principled level.

Sunstein's constitutionalist critique on rules needs to be well understood. Sometimes consensus on a specific rule is all you can get. Such arrangements might do the ordinary work, but are unfit for constitutionalisation.

That does not mean that rules have no place in a constitutionalist perspective. The level of trust required for a delicate political process, such as in the European Union (partly a process of constitutionalisation), requires going beyond principled consensus (for instance about rights) and seeking rule consensus. The trust and level of convergence needed for such an endeavor can simply not be based on principled consensus alone.⁴³ So in a certain regard, rule convergence creates a more fertile constitutional humus as opposed to some 'easy' references to principles that seem to float in the air. Ideally, at least for the constitutional quality of the humus, these rules are made by the political bodies of the EU, not by the judges. Ola Zetterquist in particular has voiced this point: the political bodies of the EU should be the main drivers of this process of seeking rule consensus and should not be leaving this to judicial law-making by the CJEU, as is regrettably too often the case in recent times. Today's EU is not about the shape of cucumbers any longer, Zetterquist argues, but about important values in need of rule operationalisation. Judicial pro-activeness has worked in the era of cucumbers but in a

40 Cass R Sunstein, 'Incompletely Theorized Agreements' (1995) 108(7) *Harvard Law Review* 1733-1772; Cass R Sunstein, 'Incompletely Theorized Agreements in Constitutional Law' (Chicago Public Law and Legal Theory Working Papers, 2007) <<http://bit.ly/2wd4mbt>> accessed 19 July 2017.

41 Sunstein, 'Incompletely Theorized Agreements in Constitutional Law' (n 40) 2.

42 *ibid* 17.

43 Compare with these considerations taken from the Preamble of the 2010 Directive on the right to interpretation and translation in criminal proceedings (OJ L 280/1-7): '(6) Although all the Member States are party to the ECHR, experience has shown that that alone does not always provide a sufficient degree of trust in the criminal justice systems of other Member States. (7) Strengthening mutual trust requires a more consistent implementation of the rights and guarantees set out in Article 6 of the ECHR. It also requires, by means of this Directive and other measures, further development within the Union of the minimum standards set out in the ECHR and the Charter'.

value-grounded Union the CJEU should reconsider its lawmaking role.⁴⁴ I recall that in my previous foreword I assessed critically the role of the CJEU and of non-political bodies such as Data Protection Authorities in shaping EU data protection law and the impossibility, created by the CJEU, for national political actors to offer rule-based guidance.⁴⁵ What is lost, or at least delegated light-footedly, is the political direction. But let me return to my main theme.

Between Seeking Principled Consensus and Rule Consensus

A conclusion of the foregoing might be that approaches seeking consensus on the basis of principles and approaches seeking rule-based consensus need to be combined, or alternated. Two illustrations.

First, the international harmonisation of data protection law and principles. Kuner points at two important hurdles. A lack of consensus on who should be the driving actor of such a harmonisation process,⁴⁶ and a lack of substantive consensus. To solve the latter via an international framework will not be easy, Kuner observes, since it would be necessary to agree on the level at which such standards should be enacted:

if they are too abstract, they may not be able to protect personal data in practice, while any standards that are too detailed may be difficult to implement locally, given the differences in legal cultures around the world. Thus far, most international initiatives concerning data protection set the agenda and formulate broad principles, but do not specify how they are to be implemented in detail.⁴⁷

The observation leaves no doubt about rule consensus as the missing link in international data privacy law.

44 Zetterquist (n 28) 13: 'In accordance with the republican ideal it primarily corresponds to the political bodies of the EU to reason on the more precise meanings of these rights and their interrelation, thereby striking the proper balance. Should the political bodies shun the issue of deliberation on fundamental values found in the Charter, this does not mean that the conflict between these various values goes away. It most likely means that they will instead end up in more or less willing courts for dispute resolution and the political fall-out from such a judgement can be quite severe. Judicial pro-activeness has played a decisive role in the making of the EC/EU, as the process of constitutionalisation shows, but the issues dealt with today are no longer on the shape of cucumbers, tariffs on chemicals or milk quotas. Today the competences of the EU stretch into the domain of criminal law and the core notions of public power. There is a therefore a need for politicization of the EU that matches the previous process of legalization. Once such a process has taken place the EUCJ can take one step back in its judicial law-making but will still have the paramount function of assessing whether these rights have been respected in the sense that any restriction must be able to pass the test of reference of the common good, the *res publica*, of the EU'.

45 De Hert, 'Data Protection's Future without Democratic Bright Line Rules' (n 12).

46 Christopher Kuner, 'The European Union and the Search for an International Data Protection Framework' (2014) 2(2) Groningen Journal of International Law 59-60: 'there is no consensus as to which international organization could coordinate the work. Indeed, in the author's experience most international organisations are wary of beginning work on a legally binding data protection instrument because of the political difficulties of reaching agreement, and would hesitate to do so failing a clear mandate from their members. While the UN has the necessary global membership, the work of legal harmonisation bodies such as the United Nations Commission on International Trade Law (UNCITRAL) demonstrates that in the highly politicised atmosphere of the UN, harmonisation even of technical topics tends to proceed slowly and with difficulty. The UN also lacks detailed expertise in the field of data protection. Thus, the possibility of a global, legally binding data protection instrument being enacted in the foreseeable future remains elusive'. See also Paul De Hert and Vagelis Papakonstantinou, 'Moving Beyond the Special Rapporteur on Privacy with the Establishment of a New, Specialised United Nations Agency: Addressing the Deficit in Global Cooperation for the Protection of Data Privacy' in Dan Jerker Swantesson and Dariusz Kloza (eds), *Trans-Atlantic Data Privacy Relations as a Challenge for Democracy* (Intersentia 2017) 521-533.

47 Kuner (n 46) 59-60.

This brings us to a second illustration about the rule and principle conundrum: EU data protection law. This regional arrangement of data protection principles has been influential in a global context in two ways: first, by serving as a model for the enactment of data protection law in other regions, and second, by its extraterritorial application to data processing in third countries.⁴⁸ But also the success within Europe of the EU regulatory options is noteworthy. Much has been said about the length of the 2016 General Data Protection Regulation (GDPR) and other recent EU data protection laws as compared to the 1995 Data Protection Directive and even more so when compared to the 1980 Council of Europe Data Protection Convention. Some see the extra pages as a sign of weakness and lack of capacity to trust the sacred principles. In my view, EU Data protection laws become bundles of principles, general rights, concrete subjective rights *and* rules. As a proponent of hardening of principles into concrete things (rules and subjective rights) by political bodies, I see in principle no error in the length of these laws. The model has definitely big appeal, to the degree that an organisation like the Council of Europe is changing course. In its reform process it is swapping its principle-based regulatory approach to data protection for the more mixed approach,⁴⁹ by adding so much EU-inspired detail in the new proposal that one can fear for the ambition of the Council of Europe to be a global regulatory player.⁵⁰

Data Protection As a Bundle of Principles and Rights and Rules, All Affected by the Reform

I observed *above* that the move in EU data protection law from a Directive towards a Regulation was partly mandated by the principle of free flow of data in the internal market. This principle required more hardened rules that are applicable in a similar way across the union. Hence the necessity for a Regulation with more detailed provisions.

This is however only one explanation amongst others and one that erroneously suggest that the bulk of the EU reform has been in norm creation at the level of rules. But the reform has done much more and has impacted all ingredients of the Directive: rules, rights (either general or subjective) *and* principles.⁵¹

Article 5 GDPR ('Principles relating to processing of personal data') is a slightly enriched copy-paste of Article 6 of the Directive suggesting a solid *acquis* that continues

48 *ibid* 61. See also Michael Birnhack, 'The EU Data Protection Directive: An Engine of a Global Regime' (2008) 24(6) Computer Law & Security Report 508–520.

49 Paul De Hert and Vagelis Papakonstantinou, 'The Council of Europe Data Protection Convention reform: Analysis of the new text and critical comment on its global ambition' (2014) 30(6) Computer Law & Security Review: The International Journal of Technology Law and Practice 633–642. See also, Sophie Kwasny, 'Convention 108, a Trans-Atlantic DNA?' in Dan Jerker Swantesson and Dariusz Kloza (eds), *Trans-Atlantic Data Privacy Relations as a Challenge for Democracy* (Intersentia 2017) 533–544.

50 Compare, Council of Europe, *Explanatory Report to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, Strasbourg (28 January 1981), para 24 <https://rm.coe.int/16800ca434> accessed 21 July 2017: 'The title describes this instrument as *Convention*, not as *European Convention* in order better to underline that there ought to be ample scope for accession to it by non-European States.'

51 Paul De Hert et al, 'Principles and the Proposed New Data Protection Regulation' (2012) 26(1) Innovation. The European Journal for Social Science Research 1–12.

to hold a central place in personal data processing. Added to this list are two ‘new’ principles, this of ‘integrity and confidentiality’ [Article 5.1(f) GDPR] and of ‘accountability’ (Article 5.2 GDPR). The principle that personal data should be processed ‘fairly and lawfully’ [Article 6.1(a) Directive] is rewritten (‘lawfully, lawfully and in a transparent manner’) and labeled as a principle of lawfulness, fairness and transparency [Article 5.1(a) GDPR]. The principle that personal data should be ‘adequate, relevant and not excessive’ [Article 6.1(c) Directive] is rewritten (‘adequate, relevant and limited to what is necessary’) and labeled as a principle of data minimisation [Article 5.1(c) GDPR].

Contrary to the OECD document and the UK Data Protection Act 1998 (see *above*) the EU documents do not recognize as such ‘internationally oriented’ principles, but the rules regarding this matter remain the same: data exports to third countries continue to require the ‘adequacy’ criterion.

The above shows continuity and partial reform in the GDPR with regard to principles. The same is the case with the set of individual data protection rights: the rights to information, access to one’s personal data and rectification are substantially reinforced, in order to deal with contemporary complexity. The introduction of a ‘right to be forgotten’ is probably the best example of a novelty in the category of rights.

Rules regarding the notification system are abolished and replaced by data controller accountability rules, a system of prior notifications whenever needed and the establishment of data protection officers in organisations with more than 250 employees. Amongst the novelties here are the introduction of mandatory data protection impact assessments (following the example of environmental law), data breach notification and ‘privacy-by-design’ obligations. Another important rule change has occurred in the chapter with regard to the sanctions and the powers of the data protection authorities.

In 2016, this journal published a short analysis of the positive elements (novelties, reinforcements and clarifications) by Simon Davies, who did not hesitate to mention the shortcomings and missed opportunities of the reform.⁵² Davies’ very concise but complete overview of good and bad, the title of his contribution (‘A Triumph of Pragmatism over Principle?’) and some of his well-chosen depictions (‘the GDPR as a creature of consensus, part Directive and part Regulation’) makes his contribution a must-read and allows me to move ahead and focus on the fact that principles can be freely chosen, created and reinforced.

Principles Are Man-Made and Political

In the above, we discussed the impact of the GDPR on the data protection principles. We found continuity and partial reform (two new principles and two rewritten, rein-

52 Simon Davies, ‘The Data Protection Regulation: A Triumph of Pragmatism over Principle?’ (2016) 2(3) EDPL 290-296.

forced principles). We also saw other ways of counting, organising and representing data protection law principles, for instance, as done in the OECD principles and in the UK Data Protection Act 1998.

Whatever the text at hand, the way these principles are presented serves similar purposes. The principles carry the data protection architecture. They are intended to be all-encompassing, abstract and omnipresent throughout the text. They make data protection robust and time-resistant. Especially in Europe this seems to be a major concern. Regardless of the outcome of the EU data protection framework amendment process and the ultimate wording of the instruments that compose it, the application and visibility of these principles ought to remain unaffected. Hence, the copy paste exercise with, at least for the eye) only minor changes and revisions. So the principles are never put directly into question, if there is a problem or a concern then this relates to the rules or to the enforcement of the principles.⁵³

This process of prioritising continuity over change is not uniquely European. When the OECD intended to revise its 1980 Guidelines, it made use of an expert group that prepared the 2013 reform of the Guidelines.

The report of the expert group contains a straightforward questioning of traditional principles and corner-stones of data protection law (the role of consent, the role of the data subject, the role of purpose specification and use limitation and even the definition of personal data), but eventually it was decided to do nothing at this stage and to leave intact the eight ‘basic principles of national application’ from the 1980 Guidelines, as well as the definitions of key terms like ‘data controller’ and ‘personal data’.⁵⁴

Both the number of principles and rights are subject to evolution. Principles and rights can be added, reinforced or even weakened (at a point of becoming obsolete). So principles and rights are work in progress, man-made not God-given.⁵⁵ The history of consent (as a right or principle) is bendy to say the least, with less visibility in the GDPR when compared to the Directive that made a great fuss about it. Trends in the formulation of principles have nothing to do with vitality or strength. The EU now reinforces data minimisation as a principle while the OECD expert group seemingly wanted to bury the principle in an era of Big Data processing. Article 8 of the EU Charter on Fun-

53 Compare, LRDP Kantor Ltd (Leader), *Comparative Study on Different Approaches to new Privacy Challenges, in Particular in the Light of Technological Developments* (2010) 15 http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf accessed 21 July 2017: ‘The basic data protection principles, rules and criteria, as developed in Europe by the COE and the EU, and as also broadly endorsed globally, in particular by the OECD, as such, have stood the test of time, even if they may need strengthening in some respects. It is a testimony to their wide acceptance that they are increasingly adopted as the basis for legislation in many parts of the world, including Asia and Africa. (...) However, their specific application and enforcement has been much less successful’.

54 ‘The proposals by the Expert Group leave intact the eight “basic principles of national application” intact as reflected in Part Two of the 1980 Guidelines, as well as the definitions of key terms like “data controller” and “personal data”. While the group has considered many issues that implicate these core principles and terms (see below), no clear direction emerged as to what changes might be needed at this stage.’ [OECD, ‘Privacy Expert Group Report on the Review of the 1980 OECD Privacy Guidelines’ (OECD Digital Economy Papers No 229, OECD Publishing 2013) 6 <<http://dx.doi.org/10.1787/5k3xz5zmj2mx-en>> accessed 21 July 2017].

55 The OECD Guidelines, for instance, were proposed as minimum standards, capable of being supplemented by additional measures. See Wright, De Hert and Gutwirth (n 35).

damental Rights, recognising the right to protection of personal data, enumerates only some of the principles and calls them ‘rules’.⁵⁶ Amusingly, consent is mentioned and data minimisation is not. Article 16 of the Treaty on the Functioning of the European Union (TFEU) is even more silent on the principles of EU data protection law and focusses on giving the EU a strong mandate for rule making.⁵⁷ Notwithstanding their selectiveness or silence on principles, both provisions make a case for the control by independent authorities.

Probably one of the most man-made and political of all principles is this principle of independent supervisory authorities. Although the OECD Guidelines do not include the principle of the establishment of a national supervisory data protection authority, the Data Protection Directive explicitly adopts it in Article 28, without including it in the list of principles contained in Article 6. A similar set-up is found in the GDPR. The cannon-ball firing of the principle in Article 8 of the Charter and Article 16 TFEU is plainly political, positioning the EU as a first league player in the field, since US law does not include any constitutional or general requirement to set up an independent national data protection authority or authorities. On that point, the US and many other countries endorse the OECD Guidelines, while Europe provides for a more stringent principle.⁵⁸

The ‘trick’ seems to work well. Most European data protection proponents insist on the principle as indispensable, obviously neglecting the ‘higher’ principle at play behind this data protection principle. This higher principle is of course contained in Article 13 of the European Convention on Human Rights recognising a right to an effective remedy,⁵⁹ without mentioning the requirement of independence. In the case of the EU Charter, the choice of principle is not inspired by seeking consensus, but by the desire to demonstrate dissidence and difference. Am I the only EU citizen disappointed by the drafting of Article 8 of the Charter and Article 16 TFEU? The pick of principles is a disgrace. Consent is introduced in one of the provisions as a principle, although it is not mentioned as a principle in the OECD and Council of Europe text and is reduced

56 art 8 of the Charter (Protection of personal data): ‘1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority’.

57 art 16 TFEU: ‘1. Everyone has the right to the protection of personal data concerning them. 2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities. The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on European Union’.

58 Compare, OECD, ‘Report on the Cross-Border Enforcement of Privacy Laws’ (2006) <<http://www.oecd.org/sti/economy/37558845.pdf>> accessed 21 July 2017: ‘If member country authorities share commonalities in terms of the powers they have and the scope of the laws they enforce, certain variations remain. Some authorities are charged with resolving individual complaints, others with supervising regulatory compliance, and many do both. Variations exist with respect to complaint handling processes, the authority to investigate or audit, and the available sanctions and remedies for a breach. Some are independent authorities, some housed within government departments. Some cover the public sphere, others only the private sector, and many cover both. A few authorities are mandated to enforce privacy laws covering a particular economic sector, for example, telecommunications or financial services’.

59 ‘Everyone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity’. See for a similar provision, art 47 of the EU Charter.

in importance in the GDPR (when compared to the Directive). The only principle that made it in the two provisions (about oversight) has undergone a *hardening* process that makes it suitable for a political pamphlet but unfit for a sacred text devoted to higher values and principles. I do not care whether the oversight is done by an *independent* body or not, as long as it is *effective* and does not block the way to the courts. The principle we need is this of an effective remedy. Independence helps or could help but is something else.

Using Principles to Define Data Protection Law (Bygrave)

Before we embarked on exploring the concepts of principles, rights and rules, I briefly mentioned Lee Bygrave's approach to data protection. This author first identifies six core principles (*fair and lawful processing; minimality; purpose limitation; data quality; data security and data subject influence*) and then argues that there might be other principles in data protection law, but these six 'are central to it', *they are data protection law*:

These are not the only principles found in data privacy law but they are central to it. More general principles not specific to the field come into play too. The proportionality principle is an example, particularly with respect to EU law. Elements of the above principles and some of the rights to which they give rise are also found outside data privacy law, for instance in legislation on freedom of information (FOI)—that is, legislation enabling public access to government-held information. Yet only legal instruments embracing all or most of the above principles are commonly considered as data privacy law—a line also taken in this book.⁶⁰

As much as I like the *data protection as a bundle of principles*-idea - in a next editorial I will compare it favorably with an alternative idea about data protection law being based on core values, I am probably not the only one that senses that Bygrave is struggling with it. Principles come and go and principles are seldom unique or autonomous. The data protection data principles are no exception. A recent report written by four professors in administrative law on *The General Principles of EU Administrative Procedural Law*, can help me to make my point.⁶¹ The four professors go to great lengths to avoid spelling out what these principles are. Only at the end of the report, one finds a list of twenty principles, preceded by the message that this list does not want to codify, but solely enunciate the general principles of EU administrative law. Codification of these principles in, for instance, a Regulation, is simply not an option. The authors refer to only partially successful attempts to summarise the principles of the right to good administration in Article 41 of the EU Charter. Not everything can be captured by including it under a principle (one might lose out of sight certain essential rules or subjective rights that do not fit a list of selected principles) and there

⁶⁰ Bygrave, *Data Privacy Law, an International Perspective* (n 20) 2.

⁶¹ Diana-Urania Galetta et al, *The General Principles of EU Administrative Procedural Law. In-depth Analysis* (European Parliament 2015) <<http://www.europarl.europa.eu/supporting-analyses>> accessed 21 July 2017.

is no clarity about what principle or aspect of principle should be seen as fundamental.⁶²

Hence my intuition that data protection should preferably be approached as a *bundle of principles, rights (general or subjective) and rules*. Even more correct is to speak about *data protection laws as bundles of principles, rights (general or subjective) and rules*. These portrayals have the double merit of a) avoiding a one-sided focus on principles that can cause neglect for certain self-standing rules or rights and b) underlining that the data protection cooking is always done using fresh ingredients and *à la carte*. One commentator discussing the draft ePrivacy Regulation, currently negotiated in Brussels, notes no less than twenty ‘points that catch the eye’, often departures of the GDPR or on the contrary rapprochements.⁶³ Everything seems possible when data protection laws are negotiated: ‘protecting natural persons or also legal persons?’; ‘reducing the possibility of consent or maximalizing it?’; ‘opening up to legitimate interest balancing or avoiding it?’, ‘protecting personal data only or other types of data too?’. Have your pick, nothing seems to be sacred.

Returning to the report on *The General Principles of EU Administrative Procedural Law*, I would like to make a second point. As mentioned, twenty principles were identified, amongst which data protection and data quality! Here is the list: *access to information and access to documents; access to the file; duty of care; data protection; data quality; effective remedy; equal treatment and non-discrimination; fair hearing; fairness; good administration; impartiality; legal certainty; legality; legitimate expectations; participatory democracy; proportionality; reason giving; rule of law; timeliness and transparency*.

Panic and a strange feeling of exhaustion overwhelms the data protection trained reader. Nothing is left of what makes data protection unique when going through the analysis of these principles. The discussion in the report of the principles of data protection and of data quality is short and does not bring about anything more than that the principle of data protection is a mixture of two other principles taken from the list: data quality salted with transparency.

Is this all the administrative law professors could come up with? (‘Public authorities need to protect personal data and keep track of their use of it’). This analysis is extremely disappointing and reductive for data protection. Still, one also has the feeling that the data subject is not deprived of many essentials when all the twenty principles are applied to his case. As a matter of fact, when rereading the twenty principles one

62 *ibid* 13: ‘Trying to exhaustively codify the fundamental principles of good administration in the operative part of a regulation would be counterproductive to the objective of Article 41 Charter on the right to good administration. The objective of adding Article 41 to the Charter was to codify some of the most important principles of good administration and to give them the status of a fundamental right. The experience of the Convention of 2000 drafting the Charter further shows how difficult it is not only to make a choice between principles in order to determine which ones are fundamental (hence the word “includes”) but also how to have a wording that reflects the variety of expressions in case-law, primary and secondary law’.

63 Gabriela Zanfir-Fortuna, ‘Highlights of the draft LIBE report on the ePrivacy Reg’ (*pdpecho*, 27 June 2017) <<https://pdpecho.com/2017/06/17/highlights-of-the-draft-libe-report-on-the-eprivacy-reg/>> accessed 21 July 2017.

gets the sensory impulse that data protection as a bundle of principles is actually no more than a small part of EU administrative procedural law! What is the data subject missing when he falls back on these twenty principles as opposed to the eight OECD principles and the six Bygrave principles? I fail to see the discomfort. On the contrary, I see much more good for the data subject relying on these twenty procedural values that take into account not only the fact that processing of personal data is amongst us, but also consider a bigger picture that includes power considerations, democracy, the need for checks on power and so forth. Why any longer turning to data protection principles and Article 8 of the Charter, when there are these principles, superior in reach, and Article 41 of the Charter?

In a next foreword, I want to come back to this bewildering experience where I am losing my familiar relationship with data protection law when reading about procedural principles in other legal domains. I will then explore further the core substance, or is it core emptiness, of data protection law. Murakami's landscape of mediums, empty shells and ghosts (either living or dead, good or bad) will continue to serve as an interpretative framework. Currently, at least at the moment of writing this contribution, I still do not understand fully the Murakami-inspired message about our data protection laws that do not know about substance and prohibitive bright-line rules.

What I do see at this moment is that data protection evolves at the level of principles, rights and rules. Data protection has given itself a past, built upon untrustworthy memories about stable principles, that guides us through the enduring cycles of reform. These memories are untrustworthy since principles in data protection law have proven to be unstable, controversial or unprecedented. If something has some importance, call it a principle.

Nothing indicates that this pretending will stop. Data protection has no vision of the future. It is loosely organised around certain unfixed principles but it has no desire to fully realise these principles. Data minimisation at one point is called a principle, and at another point is erased from our memory or handbook for the future. The question is not *does a data protection arrangement realise a given principle?* The question is rather *is this data protection arrangement conceived in such a way that a given principle in part or wholly can be attained?* The other question is necessarily *what else but principles are in a given bundle? what rights and which rules are we ignoring when we try to reduce a given data protection arrangement to a system of principles?*

(to be continued)